Amendments to the Claims:

The following Listing of the Claims replaces all prior versions, and listings, of the Claims in this Application.

Listing of Claims:

1. (canceled)

2. (canceled)

3. (canceled)

4. (canceled)

5. (canceled)

6. (amended) A method for encrypting data comprising:

broadcasting a random symbol sequence having significantly greater than N bits;

broadcasting a synchronization signal;

generating a private key;

providing said private key to an encryption station and to a decryption station;

receiving said random number sequence at said encryption station and said decryption station;

receiving said synchronization signal at said encryption station and at said decryption station;

selecting at time t a ~~an encrypting~~ subsequence from said random number sequence received at said encryption station, said selection time T based on said synchronization signal received at said encryption station and on said private key;

filling an encryption reservoir with data from said subsequence;

updating a bit count of said encryption reservoir in accordance with said filling;

generating another selection time T' based on at least said first encrypting subsequence;

selecting at time T' another subsequence from said random number sequence received at said encryption station;

additionally filling said encryption reservoir with data from said another subsequence;

updating said bit count of said encryption reservoir based on said further filling;

updating said selection time T' to represent a future time, based on at least said another subsequence;

repeating said selecting at time T', said additional filling, said updating said encryption reservoir bit count, and said updating said selection time T' until said encryption reservoir bit count reaches a predetermined fill value based on a predetermined value N;

establishing an N-bit encryption key based on said encryption reservoir;

providing a message symbol sequence to said encryption station;

encrypting said message symbol sequence, at said encryption station, based on said N-bit encrypting key ~~subsequence~~, into an encrypted symbol sequence.

7. (amended) A method for encrypting data according to claim 6, further comprising:

generating an N-bit decrypting key at said decryption station, identical to said N-bit encrypting key, said generating including

(a) selecting at said time T' said subsequence from said random number sequence received at said decryption station, said selection time T' based on said synchronization signal received at said decryption station and on said private key,

(b) filling a decryption reservoir with data from said subsequence;

(c) updating a bit count of said decryption reservoir in accordance with said filling,

(d) generating another selection time T' based on at least said subsequence,

(e) selecting at time T' another subsequence from said random number sequence received at said decryption station,

(f) additionally filling said decryption reservoir with data from said another subsequence,

(g) updating said bit count of said decryption reservoir based on said further filling,

(h) updating said selection time T' to represent a future time, based on at least said another subsequence,

(i) repeating (e) through (h) until said decryption reservoir bit count reaches a predetermined fill value based on a predetermined value N, and

(j) establishing an N-bit decryption key based on said decryption reservoir;

transmitting said encrypted symbol sequence from said encryption station to said decryption station;

~~selecting at the decryption station a decryption subsequence from the random number sequence, the boundaries of said decryption subsequence based on the private key, the selection being such that the decryption subsequence is identical to said encryption subsequence;~~

decrypting said encrypted symbol sequence, at said decryption station, based on said decrypting key ~~subsequence~~, into said message symbol sequence.

8. (new) A method according to claim 7, wherein said synchronization signal is embedded in said broadcast random number sequence.

9. (new) A method for generating an N-bit encrypting key, comprising:

broadcasting a random symbol sequence having significantly greater than N bits;

generating a private key;

providing said private key to an encrypting station;

receiving said random number sequence at said encryption station;

generating an encrypting station sampling start time T based on said private key;

sampling a plurality of bits from said random number sequence received at said encrypting station, over a time interval based on said encrypting station sampling start time T, said plurality being less than N bits;

filling an encryption key reservoir at said data encryption station based on said sampled plurality of bits;

generating an updated encrypting station start time T', based on at least said plurality of bits;

sampling another plurality of bits from said random number sequence received at said encrypting station, over a time interval based on said updated encrypting station sampling start time T', said plurality being less than N bits;

further filling said encryption key reservoir based on said another plurality of bits from said transmitted random number sequence;

repeating said generating an updated encrypting station start time T', said sampling another plurality of bits, and said further filling said encryption key reservoir until said encryption key reservoir reaches a predetermined bit count based on N; and

setting said N-bit encrypting key based on said encryption key reservoir.

10. (new) A method according to claim 9, further comprising generating an N-bit decrypting key identical in value to said N-bit encrypting key, said generating comprising:

providing said private key to a decrypting station;

receiving said random number sequence at said decryption station;

generating a decrypting station sampling start time TD based on said private key, said generating performed such that said decrypting sampling start time TD is substantially identical to said encrypting sampling start time T;

sampling a plurality of bits from said random number sequence received at decrypting station, over a time interval based on said decrypting station sampling start time TD, said plurality being less than N bits;

filling a decryption key reservoir at said data decryption station based on said sampled plurality of bits;

generating an updated decrypting station sampling start time TD', based on at least said plurality of bits;

sampling another plurality of bits from said random number sequence received at said decrypting station, over a time interval based on said updated decrypting station sampling start time TD', said plurality being less than N bits;

further filling said decryption key reservoir based on said another plurality of sampled bits;

repeating said generating an updated decrypting station sampling start time TD', said sampling another plurality of bits, and said further filling said decryption key reservoir until said decryption key reservoir reaches a predetermined bit count based on N bits; and

setting said N-bit decrypting key based on a value of said decrypting key reservoir,

wherein said generating a decrypting station sampling start time TD, said filling a decryption key reservoir, said generating an updated decrypting station sampling start time TD', said further filling said decryption key reservoir, and said repeating are performed such that said decryption key reservoir and said encryption key reservoir are identically filled.

11. (new) A method according to claim 9, further comprising

inputting a block of information into said encrypting station;

encrypting said block of information based on said N-bit encrypting key into an encrypted block of information;

transmitting said encrypted block of information from said encrypting station to said decrypting station; and

decrypting said encrypted block of information at said decrypting station based on said N-bit decrypting key.

12. (new) A method according to claim 9, further including:

generating a synchronization signal; and

receiving said synchronization signal at said encryption station,

wherein said sampling a plurality of bits is further based on said received synchronization signal.

13. (new) A method according to 10, further including:

generating a synchronization signal; and

receiving said synchronization signal at at least one of said encryption station and said decryption station,

wherein at least one of said sampling a plurality of bits at said encryption station and said decryption station is further based on said received synchronization signal.

14. (new) A method according to claim 6 wherein said transmitting the random number sequence includes:

transmitting said random number sequence by uplink up to a satellite; and

transmitting said random number sequence received by said satellite down to said encryption station and to said decryption station.

15. (new) A method according to claim 7 wherein said transmitting the random number sequence includes:

transmitting said random number sequence by uplink up to a satellite; and

transmitting said random number sequence received by said satellite down to said encryption station and to said decryption station.

16. (new) A method according to claim 8 wherein said transmitting the random number sequence with embedded synchronization signal includes:

transmitting said random number sequence and embedded synchronization signal via uplink up to a satellite; and

transmitting said random number sequence received by said satellite down to said encryption station and to said decryption station.

17. (new) A method according to claim 12 wherein said transmitting the random number sequence with embedded synchronization signal includes:

transmitting said random number sequence and embedded synchronization signal via uplink up to a satellite; and

transmitting said random number sequence received by said satellite down to said encryption station and to said decryption station.

18. (new) A method for encrypting data, comprising:

broadcasting a random number sequence having significantly greater than N bits;

providing a private key to a first communication station;

receiving said random number sequence at said first communication station;

repeatedly filling a first reservoir at said first communication station with selected bits from said received random number sequence, each selection based on at least one of said private key and a value of previously selected bits, until said first reservoir reaches a predetermined threshold based on N;

setting an N-bit encryption key based on the content of said first reservoir; and

inputting an information data;

encrypting said information data into an encrypted data based on said N-bit encryption key.

19. (new) A method according to claim 18, further comprising:

providing said private key to a first communication station;

receiving said random number sequence at said second communication station;

repeatedly filling a second reservoir at said second communication station with selected bits from said received random number sequence, each selection based on at least one of said private key and a value of previously selected bits, until said first reservoir reaches a predetermined threshold based on N, wherein said repeated filling and selection are carried out such that said second reservoir is filled to match said filling of said first reservoir;

setting an N-bit decryption key based on the content of said second reservoir, whereby said N-bit decryption key matches said N-bit encryption key;

receiving said encrypted data; and

decrypting said encrypted data based on said N-bit decryption key.